Q0001

Web・アプリケーション
タグ：反射型XSS
用語：反射型XSSの確認ポイント1：要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性

次の説明に最も合う用語はどれか。要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性

A. 反射型XSS
B. 格納型XSS
C. CSRF
D. OSコマンドインジェクション

答え・解説

Q0001 正答：A. 反射型XSS

解説：反射型XSSは、要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性。ほかの選択肢は目的又は適用場面が異なる。

Q0002

Web・アプリケーション
タグ：反射型XSS
用語：反射型XSSの確認ポイント2：要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性

反射型XSSの説明として最も適切なものはどれか。

A. 保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性
B. 要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性
C. 利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃
D. 入力をOSコマンドへ混入させ不正な命令を実行させる攻撃

答え・解説

Q0002 正答：B. 要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性

解説：反射型XSSの要点は「要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0003

Web・アプリケーション
タグ：反射型XSS
用語：反射型XSSの確認ポイント3：要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性

用語と説明の組合せとして適切なものはどれか。論点は「反射型XSS」である。

A. 格納型XSS：要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性
B. CSRF：要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性
C. 反射型XSS：要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性
D. OSコマンドインジェクション：要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性

答え・解説

Q0003 正答：C. 反射型XSS：要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性

解説：正しい組合せは「反射型XSS：要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0004

Web・アプリケーション
タグ：反射型XSS
用語：反射型XSSの確認ポイント4：要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性

「反射型XSS」は、要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性。

A. ○
B. ×

答え・解説

Q0004 正答：○

解説：正しい。反射型XSSは要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性。実務では対象、目的、前提条件を併せて確認する。

Q0005

Web・アプリケーション
タグ：反射型XSS
用語：反射型XSSの確認ポイント5：要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性

組織が「要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性」ために採用すべき概念又は仕組みはどれか。

A. 反射型XSS
B. 格納型XSS
C. CSRF
D. OSコマンドインジェクション

答え・解説

Q0005 正答：A. 反射型XSS

解説：この目的に対応するのは反射型XSSである。要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性という機能・考え方を持つためである。

Q0006

Web・アプリケーション
タグ：反射型XSS
用語：反射型XSSの確認ポイント6：要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性

「反射型XSS」について、誤解を避けるための説明として最も適切なものはどれか。

A. 入力をOSコマンドへ混入させ不正な命令を実行させる攻撃
B. 要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性
C. 利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃
D. 保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性

答え・解説

Q0006 正答：B. 要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性

解説：反射型XSSは要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0007

Web・アプリケーション
タグ：反射型XSS
用語：反射型XSSの確認ポイント7：要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性

「反射型XSS」は、保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性。

A. ○
B. ×

答え・解説

Q0007 正答：×

解説：誤り。記述は格納型XSSの説明である。反射型XSSは要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性。

Q0008

Web・アプリケーション
タグ：反射型XSS
用語：反射型XSSの確認ポイント8：要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性

次の状況で中心となる論点はどれか。「要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性」ことが求められている。

A. CSRF
B. OSコマンドインジェクション
C. 格納型XSS
D. 反射型XSS

答え・解説

Q0008 正答：D. 反射型XSS

解説：中心となる論点は反射型XSSである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0009

Web・アプリケーション
タグ：反射型XSS
用語：反射型XSSの確認ポイント9：要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性

「要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性」という特徴を持つものを選べ。

A. 反射型XSS
B. OSコマンドインジェクション
C. CSRF
D. 格納型XSS

答え・解説

Q0009 正答：A. 反射型XSS

解説：反射型XSSが該当する。定義は要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性であり、他の候補とは機能が異なる。

Q0010

Web・アプリケーション
タグ：格納型XSS
用語：格納型XSSの確認ポイント1：保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性

次の説明に最も合う用語はどれか。保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性

A. SQLインジェクション
B. 格納型XSS
C. SSRF
D. ディレクトリトラバーサル

答え・解説

Q0010 正答：B. 格納型XSS

解説：格納型XSSは、保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性。ほかの選択肢は目的又は適用場面が異なる。

Q0011

Web・アプリケーション
タグ：格納型XSS
用語：格納型XSSの確認ポイント2：保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性

格納型XSSの説明として最も適切なものはどれか。

A. 入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃
B. サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃
C. 保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性
D. パス操作により公開範囲外のファイルへアクセスする攻撃

答え・解説

Q0011 正答：C. 保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性

解説：格納型XSSの要点は「保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0012

Web・アプリケーション
タグ：格納型XSS
用語：格納型XSSの確認ポイント3：保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性

用語と説明の組合せとして適切なものはどれか。論点は「格納型XSS」である。

A. SQLインジェクション：保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性
B. SSRF：保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性
C. ディレクトリトラバーサル：保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性
D. 格納型XSS：保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性

答え・解説

Q0012 正答：D. 格納型XSS：保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性

解説：正しい組合せは「格納型XSS：保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0013

Web・アプリケーション
タグ：格納型XSS
用語：格納型XSSの確認ポイント4：保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性

「格納型XSS」は、保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性。

A. ○
B. ×

答え・解説

Q0013 正答：○

解説：正しい。格納型XSSは保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性。実務では対象、目的、前提条件を併せて確認する。

Q0014

Web・アプリケーション
タグ：格納型XSS
用語：格納型XSSの確認ポイント5：保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性

組織が「保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性」ために採用すべき概念又は仕組みはどれか。

A. SQLインジェクション
B. 格納型XSS
C. SSRF
D. ディレクトリトラバーサル

答え・解説

Q0014 正答：B. 格納型XSS

解説：この目的に対応するのは格納型XSSである。保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性という機能・考え方を持つためである。

Q0015

Web・アプリケーション
タグ：格納型XSS
用語：格納型XSSの確認ポイント6：保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性

「格納型XSS」について、誤解を避けるための説明として最も適切なものはどれか。

A. パス操作により公開範囲外のファイルへアクセスする攻撃
B. サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃
C. 保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性
D. 入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃

答え・解説

Q0015 正答：C. 保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性

解説：格納型XSSは保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0016

Web・アプリケーション
タグ：格納型XSS
用語：格納型XSSの確認ポイント7：保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性

「格納型XSS」は、入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃。

A. ○
B. ×

答え・解説

Q0016 正答：×

解説：誤り。記述はSQLインジェクションの説明である。格納型XSSは保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性。

Q0017

Web・アプリケーション
タグ：格納型XSS
用語：格納型XSSの確認ポイント8：保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性
次の状況で中心となる論点はどれか。「保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性」ことが求められている。

A. 格納型XSS
B. SSRF
C. ディレクトリトラバーサル
D. SQLインジェクション

答え・解説

Q0017 正答：A. 格納型XSS
解説：中心となる論点は格納型XSSである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0018

Web・アプリケーション
タグ：格納型XSS
用語：格納型XSSの確認ポイント9：保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性
「保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性」という特徴を持つものを選べ。

A. ディレクトリトラバーサル
B. 格納型XSS
C. SSRF
D. SQLインジェクション

答え・解説

Q0018 正答：B. 格納型XSS
解説：格納型XSSが該当する。定義は保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性であり、他の候補とは機能が異なる。

Q0019

Web・アプリケーション
タグ：SQLインジェクション
用語：SQLインジェクションの確認ポイント1：入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃

次の説明に最も合う用語はどれか。入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃

A. CSRF
B. XXE
C. SQLインジェクション
D. アクセス制御不備

答え・解説

Q0019 正答：C. SQLインジェクション

解説：SQLインジェクションは、入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃。ほかの選択肢は目的又は適用場面が異なる。

Q0020

Web・アプリケーション
タグ：SQLインジェクション
用語：SQLインジェクションの確認ポイント2：入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃

SQLインジェクションの説明として最も適切なものはどれか。

A. 利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃
B. XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃
C. 利用者が権限外の機能やデータへアクセスできる脆弱性
D. 入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃

答え・解説

Q0020 正答：D. 入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃

解説：SQLインジェクションの要点は「入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0021

Web・アプリケーション
タグ：SQLインジェクション
用語：SQLインジェクションの確認ポイント3：入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃

用語と説明の組合せとして適切なものはどれか。論点は「SQLインジェクション」である。

A. SQLインジェクション：入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃
B. CSRF：入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃
C. XXE：入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃
D. アクセス制御不備：入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃

答え・解説

Q0021 正答：A. SQLインジェクション：入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃

解説：正しい組合せは「SQLインジェクション：入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0022

Web・アプリケーション
タグ：SQLインジェクション
用語：SQLインジェクションの確認ポイント4：入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃

「SQLインジェクション」は、入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃。

A. ○
B. ×

答え・解説

Q0022 正答：○

解説：正しい。SQLインジェクションは入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃。実務では対象、目的、前提条件を併せて確認する。

Q0023

Web・アプリケーション
タグ：SQLインジェクション
用語：SQLインジェクションの確認ポイント5：入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃

組織が「入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃」ために採用すべき概念又は仕組みはどれか。

A. CSRF
B. XXE
C. SQLインジェクション
D. アクセス制御不備

答え・解説

Q0023 正答：C. SQLインジェクション

解説：この目的に対応するのはSQLインジェクションである。入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃という機能・考え方を持つためである。

Q0024

Web・アプリケーション
タグ：SQLインジェクション
用語：SQLインジェクションの確認ポイント6：入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃

「SQLインジェクション」について、誤解を避けるための説明として最も適切なものはどれか。

A. 利用者が権限外の機能やデータへアクセスできる脆弱性
B. XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃
C. 利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃
D. 入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃

答え・解説

Q0024 正答：D. 入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃

解説：SQLインジェクションは入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0025

Web・アプリケーション
タグ：SQLインジェクション
用語：SQLインジェクションの確認ポイント7：入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃

「SQLインジェクション」は、利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃。

A. ○
B. ×

答え・解説

Q0025 正答：×

解説：誤り。記述はCSRFの説明である。SQLインジェクションは入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃。

Q0026

Web・アプリケーション
タグ：SQLインジェクション
用語：SQLインジェクションの確認ポイント8：入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃

次の状況で中心となる論点はどれか。「入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃」ことが求められている。

A. XXE
B. SQLインジェクション
C. アクセス制御不備
D. CSRF

答え・解説

Q0026 正答：B. SQLインジェクション

解説：中心となる論点はSQLインジェクションである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0027

Web・アプリケーション
タグ：SQLインジェクション
用語：SQLインジェクションの確認ポイント9：入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃

「入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃」という特徴を持つものを選べ。

A. アクセス制御不備
B. XXE
C. SQLインジェクション
D. CSRF

答え・解説

Q0027 正答：C. SQLインジェクション

解説：SQLインジェクションが該当する。定義は入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃であり、他の候補とは機能が異なる。

Q0028

Web・アプリケーション
タグ：CSRF
用語：CSRFの確認ポイント1：利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃

次の説明に最も合う用語はどれか。利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃

A. SSRF
B. 安全でないデシリアライゼーション
C. 反射型XSS
D. CSRF

答え・解説

Q0028 正答：D. CSRF

解説：CSRFは、利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃。ほかの選択肢は目的又は適用場面が異なる。

Q0029

Web・アプリケーション
タグ：CSRF
用語：CSRFの確認ポイント2：利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃

CSRFの説明として最も適切なものはどれか。

A. 利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃
B. サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃
C. 信頼できない直列化データの復元により任意処理などを招く脆弱性
D. 要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性

答え・解説

Q0029 正答：A. 利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃

解説：CSRFの要点は「利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0030

Web・アプリケーション
タグ：CSRF
用語：CSRFの確認ポイント3：利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃

用語と説明の組合せとして適切なものはどれか。論点は「CSRF」である。

A. SSRF：利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃
B. CSRF：利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃
C. 安全でないデシリアライゼーション：利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃
D. 反射型XSS：利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃

答え・解説

Q0030 正答：B. CSRF：利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃

解説：正しい組合せは「CSRF：利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0031

Web・アプリケーション
タグ：CSRF
用語：CSRFの確認ポイント4：利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃

「CSRF」は、利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃。

A. ○
B. ×

答え・解説

Q0031 正答：○

解説：正しい。CSRFは利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃。実務では対象、目的、前提条件を併せて確認する。

Q0032

Web・アプリケーション
タグ：CSRF
用語：CSRFの確認ポイント5：利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃

組織が「利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃」ために採用すべき概念又は仕組みはどれか。

A. SSRF
B. 安全でないデシリアライゼーション
C. 反射型XSS
D. CSRF

答え・解説

Q0032 正答：D. CSRF

解説：この目的に対応するのはCSRFである。利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃という機能・考え方を持つためである。

Q0033

Web・アプリケーション
タグ：CSRF
用語：CSRFの確認ポイント6：利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃

「CSRF」について、誤解を避けるための説明として最も適切なものはどれか。

A. 利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃
B. 要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性
C. 信頼できない直列化データの復元により任意処理などを招く脆弱性
D. サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃

答え・解説

Q0033 正答：A. 利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃

解説：CSRFは利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0034

Web・アプリケーション
タグ：CSRF
用語：CSRFの確認ポイント7：利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃

「CSRF」は、サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃。

A. ○
B. ×

答え・解説

Q0034 正答：×

解説：誤り。記述はSSRFの説明である。CSRFは利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃。

Q0035

Web・アプリケーション
タグ：CSRF
用語：CSRFの確認ポイント8：利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃

次の状況で中心となる論点はどれか。「利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃」ことが求められている。

A. 安全でないデシリアライゼーション
B. 反射型XSS
C. CSRF
D. SSRF

答え・解説

Q0035 正答：C. CSRF

解説：中心となる論点はCSRFである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0036

Web・アプリケーション
タグ：CSRF
用語：CSRFの確認ポイント9：利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃

「利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃」という特徴を持つものを選べ。

A. 反射型XSS
B. 安全でないデシリアライゼーション
C. SSRF
D. CSRF

答え・解説

Q0036 正答：D. CSRF

解説：CSRFが該当する。定義は利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃であり、他の候補とは機能が異なる。

Q0037

Web・アプリケーション
タグ：SSRF
用語：SSRFの確認ポイント1：サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃

次の説明に最も合う用語はどれか。サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃

A. SSRF
B. XXE
C. OSコマンドインジェクション
D. 格納型XSS

答え・解説

Q0037 正答：A. SSRF

解説：SSRFは、サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃。ほかの選択肢は目的又は適用場面が異なる。

Q0038

Web・アプリケーション
タグ：SSRF
用語：SSRFの確認ポイント2：サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃

SSRFの説明として最も適切なものはどれか。

A. XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃
B. サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃
C. 入力をOSコマンドへ混入させ不正な命令を実行させる攻撃
D. 保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性

答え・解説

Q0038 正答：B. サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃

解説：SSRFの要点は「サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0039

Web・アプリケーション
タグ：SSRF
用語：SSRFの確認ポイント3：サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃

用語と説明の組合せとして適切なものはどれか。論点は「SSRF」である。

A. XXE：サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃
B. OSコマンドインジェクション：サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃
C. SSRF：サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃
D. 格納型XSS：サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃

答え・解説

Q0039 正答：C. SSRF：サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃

解説：正しい組合せは「SSRF：サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0040

Web・アプリケーション
タグ：SSRF
用語：SSRFの確認ポイント4：サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃

「SSRF」は、サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃。

A. ○
B. ×

答え・解説

Q0040 正答：○

解説：正しい。SSRFはサーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃。実務では対象、目的、前提条件を併せて確認する。

Q0041

Web・アプリケーション
タグ：SSRF
用語：SSRFの確認ポイント5：サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃

組織が「サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃」ために採用すべき概念又は仕組みはどれか。

A. SSRF
B. XXE
C. OSコマンドインジェクション
D. 格納型XSS

答え・解説

Q0041 正答：A. SSRF

解説：この目的に対応するのはSSRFである。サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃という機能・考え方を持つためである。

Q0042

Web・アプリケーション
タグ：SSRF
用語：SSRFの確認ポイント6：サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃

「SSRF」について、誤解を避けるための説明として最も適切なものはどれか。

A. 保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性
B. サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃
C. 入力をOSコマンドへ混入させ不正な命令を実行させる攻撃
D. XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃

答え・解説

Q0042 正答：B. サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃

解説：SSRFはサーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0043

Web・アプリケーション
タグ：SSRF
用語：SSRFの確認ポイント7：サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃

「SSRF」は、XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃。

A. ○
B. ×

答え・解説

Q0043 正答：×

解説：誤り。記述はXXEの説明である。SSRFはサーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃。

Q0044

Web・アプリケーション
タグ：SSRF
用語：SSRFの確認ポイント8：サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃

次の状況で中心となる論点はどれか。「サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃」ことが求められている。

A. OSコマンドインジェクション
B. 格納型XSS
C. XXE
D. SSRF

答え・解説

Q0044 正答：D. SSRF

解説：中心となる論点はSSRFである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0045

Web・アプリケーション
タグ：SSRF
用語：SSRFの確認ポイント9：サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃

「サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃」という特徴を持つものを選べ。

A. SSRF
B. 格納型XSS
C. OSコマンドインジェクション
D. XXE

答え・解説

Q0045 正答：A. SSRF

解説：SSRFが該当する。定義はサーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃であり、他の候補とは機能が異なる。

Q0046

Web・アプリケーション
タグ：XXE
用語：XXEの確認ポイント1：XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃

次の説明に最も合う用語はどれか。XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃

A. 安全でないデシリアライゼーション
B. XXE
C. ディレクトリトラバーサル
D. SQLインジェクション

答え・解説

Q0046 正答：B. XXE

解説：XXEは、XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃。ほかの選択肢は目的又は適用場面が異なる。

Q0047

Web・アプリケーション
タグ：XXE
用語：XXEの確認ポイント2：XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃

XXEの説明として最も適切なものはどれか。

A. 信頼できない直列化データの復元により任意処理などを招く脆弱性
B. パス操作により公開範囲外のファイルへアクセスする攻撃
C. XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃
D. 入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃

答え・解説

Q0047 正答：C. XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃

解説：XXEの要点は「XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0048

Web・アプリケーション
タグ：XXE
用語：XXEの確認ポイント3：XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃

用語と説明の組合せとして適切なものはどれか。論点は「XXE」である。

A. 安全でないデシリアライゼーション：XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃
B. ディレクトリトラバーサル：XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃
C. SQLインジェクション：XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃
D. XXE：XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃

答え・解説

Q0048 正答：D. XXE：XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃

解説：正しい組合せは「XXE：XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0049

Web・アプリケーション
タグ：XXE
用語：XXEの確認ポイント4：XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃
「XXE」は、XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃。

A. ○
B. ×

答え・解説

Q0049 正答：○
解説：正しい。XXEはXML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃。実務では対象、目的、前提条件を併せて確認する。

Q0050

Web・アプリケーション
タグ：XXE
用語：XXEの確認ポイント5：XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃
組織が「XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃」ために採用すべき概念又は仕組みはどれか。

A. 安全でないデシリアライゼーション
B. XXE
C. ディレクトリトラバーサル
D. SQLインジェクション

答え・解説

Q0050 正答：B. XXE
解説：この目的に対応するのはXXEである。XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃という機能・考え方を持つためである。

Q0051

Web・アプリケーション
タグ：XXE
用語：XXEの確認ポイント6：XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃

「XXE」について、誤解を避けるための説明として最も適切なものはどれか。

A. 入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃
B. パス操作により公開範囲外のファイルへアクセスする攻撃
C. XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃
D. 信頼できない直列化データの復元により任意処理などを招く脆弱性

答え・解説

Q0051 正答：C. XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃

解説：XXEはXML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0052

Web・アプリケーション
タグ：XXE
用語：XXEの確認ポイント7：XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃

「XXE」は、信頼できない直列化データの復元により任意処理などを招く脆弱性。

A. ○
B. ×

答え・解説

Q0052 正答：×

解説：誤り。記述は安全でないデシリアライゼーションの説明である。XXEはXML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃。

Q0053

Web・アプリケーション
タグ：XXE
用語：XXEの確認ポイント8：XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃
次の状況で中心となる論点はどれか。「XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃」ことが求められている。

A. XXE
B. ディレクトリトラバーサル
C. SQLインジェクション
D. 安全でないデシリアライゼーション

答え・解説

Q0053 正答：A. XXE
解説：中心となる論点はXXEである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0054

Web・アプリケーション
タグ：XXE
用語：XXEの確認ポイント9：XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃
「XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃」という特徴を持つものを選べ。

A. SQLインジェクション
B. XXE
C. ディレクトリトラバーサル
D. 安全でないデシリアライゼーション

答え・解説

Q0054 正答：B. XXE
解説：XXEが該当する。定義はXML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃であり、他の候補とは機能が異なる。

Q0055

Web・アプリケーション
タグ：安全でないデシリアライゼーション
用語：安全でないデシリアライゼーションの確認ポイント1：信頼できない直列化データの復元により任意処理などを招く脆弱性

次の説明に最も合う用語はどれか。信頼できない直列化データの復元により任意処理などを招く脆弱性

A. OSコマンドインジェクション
B. アクセス制御不備
C. 安全でないデシリアライゼーション
D. CSRF

答え・解説

Q0055 正答：C. 安全でないデシリアライゼーション

解説：安全でないデシリアライゼーションは、信頼できない直列化データの復元により任意処理などを招く脆弱性。ほかの選択肢は目的又は適用場面が異なる。

Q0056

Web・アプリケーション
タグ：安全でないデシリアライゼーション
用語：安全でないデシリアライゼーションの確認ポイント2：信頼できない直列化データの復元により任意処理などを招く脆弱性

安全でないデシリアライゼーションの説明として最も適切なものはどれか。

A. 入力をOSコマンドへ混入させ不正な命令を実行させる攻撃
B. 利用者が権限外の機能やデータへアクセスできる脆弱性
C. 利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃
D. 信頼できない直列化データの復元により任意処理などを招く脆弱性

答え・解説

Q0056 正答：D. 信頼できない直列化データの復元により任意処理などを招く脆弱性

解説：安全でないデシリアライゼーションの要点は「信頼できない直列化データの復元により任意処理などを招く脆弱性」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0057

Web・アプリケーション
タグ：安全でないデシリアライゼーション
用語：安全でないデシリアライゼーションの確認ポイント3：信頼できない直列化データの復元により任意処理などを招く脆弱性

用語と説明の組合せとして適切なものはどれか。論点は「安全でないデシリアライゼーション」である。

A. 安全でないデシリアライゼーション：信頼できない直列化データの復元により任意処理などを招く脆弱性
B. OSコマンドインジェクション：信頼できない直列化データの復元により任意処理などを招く脆弱性
C. アクセス制御不備：信頼できない直列化データの復元により任意処理などを招く脆弱性
D. CSRF：信頼できない直列化データの復元により任意処理などを招く脆弱性

答え・解説

Q0057 正答：A. 安全でないデシリアライゼーション：信頼できない直列化データの復元により任意処理などを招く脆弱性

解説：正しい組合せは「安全でないデシリアライゼーション：信頼できない直列化データの復元により任意処理などを招く脆弱性」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0058

Web・アプリケーション
タグ：安全でないデシリアライゼーション
用語：安全でないデシリアライゼーションの確認ポイント4：信頼できない直列化データの復元により任意処理などを招く脆弱性

「安全でないデシリアライゼーション」は、信頼できない直列化データの復元により任意処理などを招く脆弱性。

A. ○
B. ×

答え・解説

Q0058 正答：○

解説：正しい。安全でないデシリアライゼーションは信頼できない直列化データの復元により任意処理などを招く脆弱性。実務では対象、目的、前提条件を併せて確認する。

Q0059

Web・アプリケーション
タグ：安全でないデシリアライゼーション
用語：安全でないデシリアライゼーションの確認ポイント5：信頼できない直列化データの復元により任意処理などを招く脆弱性

組織が「信頼できない直列化データの復元により任意処理などを招く脆弱性」ために採用すべき概念又は仕組みはどれか。

A. OSコマンドインジェクション
B. アクセス制御不備
C. 安全でないデシリアライゼーション
D. CSRF

答え・解説

Q0059 正答：C. 安全でないデシリアライゼーション

解説：この目的に対応するのは安全でないデシリアライゼーションである。信頼できない直列化データの復元により任意処理などを招く脆弱性という機能・考え方を持つためである。

Q0060

Web・アプリケーション
タグ：安全でないデシリアライゼーション
用語：安全でないデシリアライゼーションの確認ポイント6：信頼できない直列化データの復元により任意処理などを招く脆弱性

「安全でないデシリアライゼーション」について、誤解を避けるための説明として最も適切なものはどれか。

A. 利用者の認証済み状態を悪用して意図しない更新要求を送らせる攻撃
B. 利用者が権限外の機能やデータへアクセスできる脆弱性
C. 入力をOSコマンドへ混入させ不正な命令を実行させる攻撃
D. 信頼できない直列化データの復元により任意処理などを招く脆弱性

答え・解説

Q0060 正答：D. 信頼できない直列化データの復元により任意処理などを招く脆弱性

解説：安全でないデシリアライゼーションは信頼できない直列化データの復元により任意処理などを招く脆弱性。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0061

Web・アプリケーション
タグ：安全でないデシリアライゼーション
用語：安全でないデシリアライゼーションの確認ポイント7：信頼できない直列化データの復元により任意処理などを招く脆弱性

「安全でないデシリアライゼーション」は、入力をOSコマンドへ混入させ不正な命令を実行させる攻撃。

A. ○
B. ×

答え・解説

Q0061 正答：×

解説：誤り。記述はOSコマンドインジェクションの説明である。安全でないデシリアライゼーションは信頼できない直列化データの復元により任意処理などを招く脆弱性。

Q0062

Web・アプリケーション
タグ：安全でないデシリアライゼーション
用語：安全でないデシリアライゼーションの確認ポイント8：信頼できない直列化データの復元により任意処理などを招く脆弱性

次の状況で中心となる論点はどれか。「信頼できない直列化データの復元により任意処理などを招く脆弱性」ことが求められている。

A. アクセス制御不備
B. 安全でないデシリアライゼーション
C. CSRF
D. OSコマンドインジェクション

答え・解説

Q0062 正答：B. 安全でないデシリアライゼーション

解説：中心となる論点は安全でないデシリアライゼーションである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0063

Web・アプリケーション
タグ：安全でないデシリアライゼーション
用語：安全でないデシリアライゼーションの確認ポイント9：信頼できない直列化データの復元により任意処理などを招く脆弱性

「信頼できない直列化データの復元により任意処理などを招く脆弱性」という特徴を持つものを選べ。

A. CSRF
B. アクセス制御不備
C. 安全でないデシリアライゼーション
D. OSコマンドインジェクション

答え・解説

Q0063 正答：C. 安全でないデシリアライゼーション

解説：安全でないデシリアライゼーションが該当する。定義は信頼できない直列化データの復元により任意処理などを招く脆弱性であり、他の候補とは機能が異なる。

Q0064

Web・アプリケーション
タグ：OSコマンドインジェクション
用語：OSコマンドインジェクションの確認ポイント1：入力をOSコマンドへ混入させ不正な命令を実行させる攻撃

次の説明に最も合う用語はどれか。入力をOSコマンドへ混入させ不正な命令を実行させる攻撃

A. ディレクトリトラバーサル
B. 反射型XSS
C. SSRF
D. OSコマンドインジェクション

答え・解説

Q0064 正答：D. OSコマンドインジェクション

解説：OSコマンドインジェクションは、入力をOSコマンドへ混入させ不正な命令を実行させる攻撃。ほかの選択肢は目的又は適用場面が異なる。

Q0065

Web・アプリケーション
タグ：OSコマンドインジェクション
用語：OSコマンドインジェクションの確認ポイント2：入力をOSコマンドへ混入させ不正な命令を実行させる攻撃

OSコマンドインジェクションの説明として最も適切なものはどれか。

A. 入力をOSコマンドへ混入させ不正な命令を実行させる攻撃
B. パス操作により公開範囲外のファイルへアクセスする攻撃
C. 要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性
D. サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃

答え・解説

Q0065 正答：A. 入力をOSコマンドへ混入させ不正な命令を実行させる攻撃

解説：OSコマンドインジェクションの要点は「入力をOSコマンドへ混入させ不正な命令を実行させる攻撃」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0066

Web・アプリケーション
タグ：OSコマンドインジェクション
用語：OSコマンドインジェクションの確認ポイント3：入力をOSコマンドへ混入させ不正な命令を実行させる攻撃

用語と説明の組合せとして適切なものはどれか。論点は「OSコマンドインジェクション」である。

A. ディレクトリトラバーサル：入力をOSコマンドへ混入させ不正な命令を実行させる攻撃
B. OSコマンドインジェクション：入力をOSコマンドへ混入させ不正な命令を実行させる攻撃
C. 反射型XSS：入力をOSコマンドへ混入させ不正な命令を実行させる攻撃
D. SSRF：入力をOSコマンドへ混入させ不正な命令を実行させる攻撃

答え・解説

Q0066 正答：B. OSコマンドインジェクション：入力をOSコマンドへ混入させ不正な命令を実行させる攻撃

解説：正しい組合せは「OSコマンドインジェクション：入力をOSコマンドへ混入させ不正な命令を実行させる攻撃」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0067

Web・アプリケーション
タグ：OSコマンドインジェクション
用語：OSコマンドインジェクションの確認ポイント4：入力をOSコマンドへ混入させ不正な命令を実行させる攻撃

「OSコマンドインジェクション」は、入力をOSコマンドへ混入させ不正な命令を実行させる攻撃。

A. ○
B. ×

答え・解説

Q0067 正答：○

解説：正しい。OSコマンドインジェクションは入力をOSコマンドへ混入させ不正な命令を実行させる攻撃。実務では対象、目的、前提条件を併せて確認する。

Q0068

Web・アプリケーション
タグ：OSコマンドインジェクション
用語：OSコマンドインジェクションの確認ポイント5：入力をOSコマンドへ混入させ不正な命令を実行させる攻撃

組織が「入力をOSコマンドへ混入させ不正な命令を実行させる攻撃」ために採用すべき概念又は仕組みはどれか。

A. ディレクトリトラバーサル
B. 反射型XSS
C. SSRF
D. OSコマンドインジェクション

答え・解説

Q0068 正答：D. OSコマンドインジェクション

解説：この目的に対応するのはOSコマンドインジェクションである。入力をOSコマンドへ混入させ不正な命令を実行させる攻撃という機能・考え方を持つためである。

Q0069

Web・アプリケーション
タグ：OSコマンドインジェクション
用語：OSコマンドインジェクションの確認ポイント6：入力をOSコマンドへ混入させ不正な命令を実行させる攻撃

「OSコマンドインジェクション」について、誤解を避けるための説明として最も適切なものはどれか。

A. 入力をOSコマンドへ混入させ不正な命令を実行させる攻撃
B. サーバに攻撃者指定のURLへアクセスさせ内部資源などを取得する攻撃
C. 要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性
D. パス操作により公開範囲外のファイルへアクセスする攻撃

答え・解説

Q0069 正答：A. 入力をOSコマンドへ混入させ不正な命令を実行させる攻撃

解説：OSコマンドインジェクションは入力をOSコマンドへ混入させ不正な命令を実行させる攻撃。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0070

Web・アプリケーション
タグ：OSコマンドインジェクション
用語：OSコマンドインジェクションの確認ポイント7：入力をOSコマンドへ混入させ不正な命令を実行させる攻撃

「OSコマンドインジェクション」は、パス操作により公開範囲外のファイルへアクセスする攻撃。

A. ○
B. ×

答え・解説

Q0070 正答：×

解説：誤り。記述はディレクトリトラバーサルの説明である。OSコマンドインジェクションは入力をOSコマンドへ混入させ不正な命令を実行させる攻撃。

Q0071

Web・アプリケーション
タグ：OSコマンドインジェクション
用語：OSコマンドインジェクションの確認ポイント8：入力をOSコマンドへ混入させ不正な命令を実行させる攻撃

次の状況で中心となる論点はどれか。「入力をOSコマンドへ混入させ不正な命令を実行させる攻撃」ことが求められている。

A. 反射型XSS
B. SSRF
C. OSコマンドインジェクション
D. ディレクトリトラバーサル

答え・解説

Q0071 正答：C. OSコマンドインジェクション

解説：中心となる論点はOSコマンドインジェクションである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0072

Web・アプリケーション
タグ：OSコマンドインジェクション
用語：OSコマンドインジェクションの確認ポイント9：入力をOSコマンドへ混入させ不正な命令を実行させる攻撃

「入力をOSコマンドへ混入させ不正な命令を実行させる攻撃」という特徴を持つものを選べ。

A. SSRF
B. 反射型XSS
C. ディレクトリトラバーサル
D. OSコマンドインジェクション

答え・解説

Q0072 正答：D. OSコマンドインジェクション

解説：OSコマンドインジェクションが該当する。定義は入力をOSコマンドへ混入させ不正な命令を実行させる攻撃であり、他の候補とは機能が異なる。

Q0073

Web・アプリケーション
タグ：ディレクトリトラバーサル
用語：ディレクトリトラバーサルの確認ポイント1：パス操作により公開範囲外のファイルへアクセスする攻撃

次の説明に最も合う用語はどれか。パス操作により公開範囲外のファイルへアクセスする攻撃

A. ディレクトリトラバーサル
B. アクセス制御不備
C. 格納型XSS
D. XXE

答え・解説

Q0073 正答：A. ディレクトリトラバーサル

解説：ディレクトリトラバーサルは、パス操作により公開範囲外のファイルへアクセスする攻撃。ほかの選択肢は目的又は適用場面が異なる。

Q0074

Web・アプリケーション
タグ：ディレクトリトラバーサル
用語：ディレクトリトラバーサルの確認ポイント2：パス操作により公開範囲外のファイルへアクセスする攻撃

ディレクトリトラバーサルの説明として最も適切なものはどれか。

A. 利用者が権限外の機能やデータへアクセスできる脆弱性
B. パス操作により公開範囲外のファイルへアクセスする攻撃
C. 保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性
D. XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃

答え・解説

Q0074 正答：B. パス操作により公開範囲外のファイルへアクセスする攻撃

解説：ディレクトリトラバーサルの要点は「パス操作により公開範囲外のファイルへアクセスする攻撃」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0075

Web・アプリケーション
タグ：ディレクトリトラバーサル
用語：ディレクトリトラバーサルの確認ポイント3：パス操作により公開範囲外のファイルへアクセスする攻撃

用語と説明の組合せとして適切なものはどれか。論点は「ディレクトリトラバーサル」である。

A. アクセス制御不備：パス操作により公開範囲外のファイルへアクセスする攻撃
B. 格納型XSS：パス操作により公開範囲外のファイルへアクセスする攻撃
C. ディレクトリトラバーサル：パス操作により公開範囲外のファイルへアクセスする攻撃
D. XXE：パス操作により公開範囲外のファイルへアクセスする攻撃

答え・解説

Q0075 正答：C. ディレクトリトラバーサル：パス操作により公開範囲外のファイルへアクセスする攻撃

解説：正しい組合せは「ディレクトリトラバーサル：パス操作により公開範囲外のファイルへアクセスする攻撃」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0076

Web・アプリケーション
タグ：ディレクトリトラバーサル
用語：ディレクトリトラバーサルの確認ポイント4：パス操作により公開範囲外のファイルへアクセスする攻撃

「ディレクトリトラバーサル」は、パス操作により公開範囲外のファイルへアクセスする攻撃。

A. ○
B. ×

答え・解説

Q0076 正答：○

解説：正しい。ディレクトリトラバーサルはパス操作により公開範囲外のファイルへアクセスする攻撃。実務では対象、目的、前提条件を併せて確認する。

Q0077

Web・アプリケーション
タグ：ディレクトリトラバーサル
用語：ディレクトリトラバーサルの確認ポイント5：パス操作により公開範囲外のファイルへアクセスする攻撃

組織が「パス操作により公開範囲外のファイルへアクセスする攻撃」ために採用すべき概念又は仕組みはどれか。

A. ディレクトリトラバーサル
B. アクセス制御不備
C. 格納型XSS
D. XXE

答え・解説

Q0077 正答：A. ディレクトリトラバーサル

解説：この目的に対応するのはディレクトリトラバーサルである。パス操作により公開範囲外のファイルへアクセスする攻撃という機能・考え方を持つためである。

Q0078

Web・アプリケーション
タグ：ディレクトリトラバーサル
用語：ディレクトリトラバーサルの確認ポイント6：パス操作により公開範囲外のファイルへアクセスする攻撃

「ディレクトリトラバーサル」について、誤解を避けるための説明として最も適切なものはどれか。

A. XML外部実体の処理を悪用してファイル読取りや外部通信を行わせる攻撃
B. パス操作により公開範囲外のファイルへアクセスする攻撃
C. 保存された不正スクリプトが他の利用者のブラウザで実行される脆弱性
D. 利用者が権限外の機能やデータへアクセスできる脆弱性

答え・解説

Q0078 正答：B. パス操作により公開範囲外のファイルへアクセスする攻撃

解説：ディレクトリトラバーサルはパス操作により公開範囲外のファイルへアクセスする攻撃。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0079

Web・アプリケーション
タグ：ディレクトリトラバーサル
用語：ディレクトリトラバーサルの確認ポイント7：パス操作により公開範囲外のファイルへアクセスする攻撃

「ディレクトリトラバーサル」は、利用者が権限外の機能やデータへアクセスできる脆弱性。

A. ○
B. ×

答え・解説

Q0079 正答：×

解説：誤り。記述はアクセス制御不備の説明である。ディレクトリトラバーサルはパス操作により公開範囲外のファイルへアクセスする攻撃。

Q0080

Web・アプリケーション
タグ：ディレクトリトラバーサル
用語：ディレクトリトラバーサルの確認ポイント8：パス操作により公開範囲外のファイルへアクセスする攻撃

次の状況で中心となる論点はどれか。「パス操作により公開範囲外のファイルへアクセスする攻撃」ことが求められている。

A. 格納型XSS
B. XXE
C. アクセス制御不備
D. ディレクトリトラバーサル

答え・解説

Q0080 正答：D. ディレクトリトラバーサル

解説：中心となる論点はディレクトリトラバーサルである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0081

Web・アプリケーション
タグ：ディレクトリトラバーサル
用語：ディレクトリトラバーサルの確認ポイント9：パス操作により公開範囲外のファイルへアクセスする攻撃

「パス操作により公開範囲外のファイルへアクセスする攻撃」という特徴を持つものを選べ。

A. ディレクトリトラバーサル
B. XXE
C. 格納型XSS
D. アクセス制御不備

答え・解説

Q0081 正答：A. ディレクトリトラバーサル

解説：ディレクトリトラバーサルが該当する。定義はパス操作により公開範囲外のファイルへアクセスする攻撃であり、他の候補とは機能が異なる。

Q0082

Web・アプリケーション
タグ：アクセス制御不備
用語：アクセス制御不備の確認ポイント1：利用者が権限外の機能やデータへアクセスできる脆弱性

次の説明に最も合う用語はどれか。利用者が権限外の機能やデータへアクセスできる脆弱性

A. 反射型XSS
B. アクセス制御不備
C. SQLインジェクション
D. 安全でないデシリアライゼーション

答え・解説

Q0082 正答：B. アクセス制御不備

解説：アクセス制御不備は、利用者が権限外の機能やデータへアクセスできる脆弱性。ほかの選択肢は目的又は適用場面が異なる。

Q0083

Web・アプリケーション
タグ：アクセス制御不備
用語：アクセス制御不備の確認ポイント2：利用者が権限外の機能やデータへアクセスできる脆弱性

アクセス制御不備の説明として最も適切なものはどれか。

A. 要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性
B. 入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃
C. 利用者が権限外の機能やデータへアクセスできる脆弱性
D. 信頼できない直列化データの復元により任意処理などを招く脆弱性

答え・解説

Q0083 正答：C. 利用者が権限外の機能やデータへアクセスできる脆弱性

解説：アクセス制御不備の要点は「利用者が権限外の機能やデータへアクセスできる脆弱性」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0084

Web・アプリケーション
タグ：アクセス制御不備
用語：アクセス制御不備の確認ポイント3：利用者が権限外の機能やデータへアクセスできる脆弱性

用語と説明の組合せとして適切なものはどれか。論点は「アクセス制御不備」である。

A. 反射型XSS：利用者が権限外の機能やデータへアクセスできる脆弱性
B. SQLインジェクション：利用者が権限外の機能やデータへアクセスできる脆弱性
C. 安全でないデシリアライゼーション：利用者が権限外の機能やデータへアクセスできる脆弱性
D. アクセス制御不備：利用者が権限外の機能やデータへアクセスできる脆弱性

答え・解説

Q0084 正答：D. アクセス制御不備：利用者が権限外の機能やデータへアクセスできる脆弱性

解説：正しい組合せは「アクセス制御不備：利用者が権限外の機能やデータへアクセスできる脆弱性」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0085

Web・アプリケーション
タグ：アクセス制御不備
用語：アクセス制御不備の確認ポイント4：利用者が権限外の機能やデータへアクセスできる脆弱性

「アクセス制御不備」は、利用者が権限外の機能やデータへアクセスできる脆弱性。

A. ○
B. ×

答え・解説

Q0085 正答：○

解説：正しい。アクセス制御不備は利用者が権限外の機能やデータへアクセスできる脆弱性。実務では対象、目的、前提条件を併せて確認する。

Q0086

Web・アプリケーション
タグ：アクセス制御不備
用語：アクセス制御不備の確認ポイント5：利用者が権限外の機能やデータへアクセスできる脆弱性

組織が「利用者が権限外の機能やデータへアクセスできる脆弱性」ために採用すべき概念又は仕組みはどれか。

A. 反射型XSS
B. アクセス制御不備
C. SQLインジェクション
D. 安全でないデシリアライゼーション

答え・解説

Q0086 正答：B. アクセス制御不備

解説：この目的に対応するのはアクセス制御不備である。利用者が権限外の機能やデータへアクセスできる脆弱性という機能・考え方を持つためである。

Q0087

Web・アプリケーション
タグ：アクセス制御不備
用語：アクセス制御不備の確認ポイント6：利用者が権限外の機能やデータへアクセスできる脆弱性

「アクセス制御不備」について、誤解を避けるための説明として最も適切なものはどれか。

A. 信頼できない直列化データの復元により任意処理などを招く脆弱性
B. 入力をSQL文の一部として解釈させ不正なデータベース操作を行う攻撃
C. 利用者が権限外の機能やデータへアクセスできる脆弱性
D. 要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性

答え・解説

Q0087 正答：C. 利用者が権限外の機能やデータへアクセスできる脆弱性

解説：アクセス制御不備は利用者が権限外の機能やデータへアクセスできる脆弱性。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0088

Web・アプリケーション
タグ：アクセス制御不備
用語：アクセス制御不備の確認ポイント7：利用者が権限外の機能やデータへアクセスできる脆弱性

「アクセス制御不備」は、要求に含まれた不正スクリプトが応答へ反映されブラウザで実行される脆弱性。

A. ○
B. ×

答え・解説

Q0088 正答：×

解説：誤り。記述は反射型XSSの説明である。アクセス制御不備は利用者が権限外の機能やデータへアクセスできる脆弱性。

Q0089

Web・アプリケーション
タグ：アクセス制御不備
用語：アクセス制御不備の確認ポイント8：利用者が権限外の機能やデータへアクセスできる脆弱性

次の状況で中心となる論点はどれか。「利用者が権限外の機能やデータへアクセスできる脆弱性」ことが求められている。

A. アクセス制御不備
B. SQLインジェクション
C. 安全でないデシリアライゼーション
D. 反射型XSS

答え・解説

Q0089 正答：A. アクセス制御不備

解説：中心となる論点はアクセス制御不備である。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0090

Web・アプリケーション
タグ：アクセス制御不備
用語：アクセス制御不備の確認ポイント9：利用者が権限外の機能やデータへアクセスできる脆弱性

「利用者が権限外の機能やデータへアクセスできる脆弱性」という特徴を持つものを選べ。

A. 安全でないデシリアライゼーション
B. アクセス制御不備
C. SQLインジェクション
D. 反射型XSS

答え・解説

Q0090 正答：B. アクセス制御不備

解説：アクセス制御不備が該当する。定義は利用者が権限外の機能やデータへアクセスできる脆弱性であり、他の候補とは機能が異なる。